

Task 1: Implementing Basic Security Scans in Azure Pipelines

Edited the existing azure-pipeline-frontend file, added SonarCloud

Azure DevOps VolodymyrDibrova0326 / MyProjectVivi / Repos / Files / fullstack-azure-app

MyProjectVivi +

- Overview
- Boards
- Repos
- Files
- Commits
- Pushes
- Branches
- Tags
- Pull requests
- Advanced Security
- Pipelines
- Test Plans
- Artifacts
- Project settings

Sonar / azure-pipelines-frontend.yml

Contents History Compare Blame

```
28 | workingDir: 'frontend/hello-azure'
29 |
30 | - task: SonarCloudPrepare@1
31 |   inputs:
32 |     SonarCloud: 'SonarQube1'
33 |     organization: 'volodymyrdibrova0326'
34 |     scannerMode: 'CLI'
35 |     cliProjectKey: 'VolodymyrDibrova0326_fullstack-azure-app'
36 |
37 | - script: |
38 |   echo "🚧 Building frontend..."
39 |   npm run build
40 |   displayName: 'Build frontend'
41 |   workingDirectory: 'frontend/hello-azure'
42 |
43 | - script: |
44 |   echo "📁 Creating coverage directory..."
45 |   mkdir -p frontend/hello-azure/coverage
46 |   displayName: 'Ensure coverage directory exists'
47 |
48 | - script: |
49 |   echo "🧪 Running Jest to generate coverage..."
50 |   npm test -- --coverage --coverageReporters=lcov
51 |   displayName: 'Run Jest tests to generate coverage'
52 |   workingDirectory: 'frontend/hello-azure'
53 |
54 | - script: |
55 |   echo "🔍 Checking if coverage report exists..."
56 |   if [ -f "frontend/hello-azure/coverage/lcov.info" ]; then
57 |     echo "✅ Coverage report found."
58 |   else
59 |     echo "❌ ERROR: Coverage report not found!"
60 |     exit 1
61 |   fi
62 |   displayName: 'Verify coverage report existence'
```

Created sonar-project.properties

Azure DevOps VolodymyrDibrova0326 / MyProjectVivi / Repos / Files / fullstack-azure-app

MyProjectVivi +

- Overview
- Boards
- Repos
- Files
- Commits
- Pushes
- Branches
- Tags
- Pull requests

Sonar / sonar-project.properties

Contents History Compare Blame

```
1 sonar.projectKey=VolodymyrDibrova0326_fullstack-azure-app
2 sonar.organization=volodymyrdibrova0326
3 sonar.host.url=https://sonarcloud.io
4
5 sonar.sources=frontend/hello-azure/src
6 sonar.sourceEncoding=UTF-8
7
8 sonar.javascript.lcov.reportPaths=frontend/hello-azure/coverage/lcov.info
9
```

Running pipeline:

The screenshot shows the Azure DevOps interface. On the left, the 'Pipelines' tab is selected, showing a list of pipelines. The main area displays the 'Run SonarCloud Analysis' pipeline run. The run status is 'Completed' with a green checkmark. The summary shows 1 run completed, 1 passed, and 0 failed. The pass percentage is 100%, the run duration is 1s 580ms, and there are 0 tests reported. The raw log shows the command line script being executed, including the SonarCloud CLI command and the output of the analysis.

Result after SonarQube

The screenshot shows the SonarQube interface. The 'fullstack-azure-app' project is selected. The 'Overall Code' tab is active, showing the following metrics:

- Security: 0 Open Issues (A)
- Reliability: 0 Open Issues (A)
- Maintainability: 0 Open Issues (A)
- Accepted Issues: 0
- Coverage: 5.0% (No conditions set on 16 Lines to cover)
- Duplications: 0.0% (No conditions set on 117 Lines)

2.

Task 2: Integrating Azure Security Center with DevOps Workflows

Objective: Configure Azure Security Center to monitor resources and integrate its alerts into Azure DevOps workflows for automated security incident response.

Steps:

- Enable Azure Security Center in your Azure subscription.
- Set up security policies and recommendations for your resources.
- Configure alerts for security incidents and integrate them with Azure DevOps using Azure Logic Apps or Azure Functions.

- Create an Azure DevOps work item automatically when a security alert is triggered.
- Test the integration by simulating a security incident and verifying that the workflow responds appropriately.

1.Enabled Azure Security Center in your Azure subscription.

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free		Full	Off On
Defender CSPM	\$5/Billable resource/Month	34 resources	Partial	Off On

Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month)	16 servers		Off On
App Service	\$15/Instance/Month	4 instances	Full	Off On
Databases	Selected 0/4	Protected: 1/1 instances	Full	Off On
Storage	\$10/Storage account/month	17 storage accounts	Full	Off On
Containers	\$5-8000/AI core/Month	1 container registries; 0 Kubernetes cores		Off On
Key Vault	\$0.25/Vault/Month	0 key vaults	Full	Off On
Resource Manager	\$5/Subscription/Month		Full	Off On

2.Set up security policies and recommendations for your resources.

Recommendations by risk

6 Critical 0 High (0) 27 Medium (27) 27 Low (27)

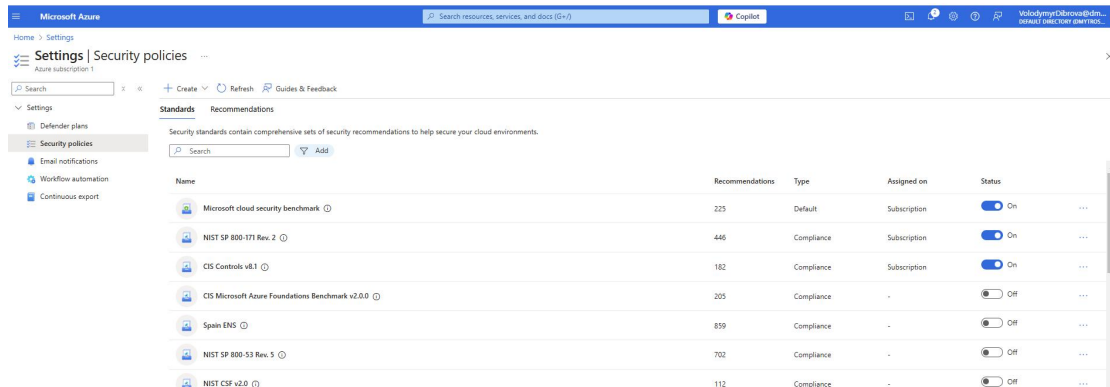
Other metrics: 0 Active attack paths, 0 Overdue recommendations

Foundational CSPM: 2 Recommendations, No risk calculated

Title	Affected resource	Risk level	Risk factors	Attack paths	Owner	Status	Insights
Storage accounts should restrict network access using virtual network rules	andribeasha96b	Critical	Critical Resource +2	0		Unassigned	
Storage accounts should restrict network access using virtual network rules	serhiperlenkoak9ee	Critical	Critical Resource +2	0		Unassigned	
Storage accounts should prevent shared key access	andribeasha96b	Critical	Critical Resource +2	0		Unassigned	
Storage accounts should prevent shared key access	serhiperlenkoak9ee	Critical	Critical Resource +2	0		Unassigned	
Storage account should use a private link connection	andribeasha96b	Critical	Critical Resource +2	0		Unassigned	
Storage accounts should prevent shared key access	test2ba	Medium	Exposure to the Internet	0		Unassigned	
Storage accounts should prevent shared key access	backendsstorage598173	Medium	Exposure to the Internet	0		Unassigned	
Storage accounts should prevent shared key access	vfstac29640	Medium	Exposure to the Internet	0		Unassigned	

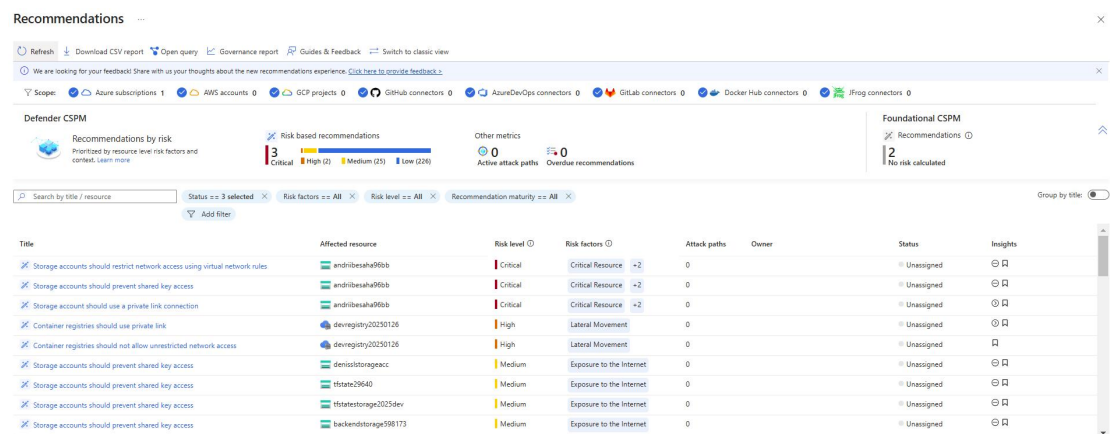
- CIS Microsoft Azure Foundations Benchmark (v2.0.0) – provides advanced security recommendations.

- NIST SP 800-53 Rev. 5 – security standard for regulatory compliance.
- CIS Controls v8.1 – general security practices.



The screenshot shows the 'Settings | Security policies' page in the Microsoft Azure portal. The left sidebar contains navigation links: Settings, Defender plans, Security policies (selected), Email notifications, Workflow automation, and Continuous export. The main content area is titled 'Standards' and 'Recommendations'. It lists several security standards with their respective recommendation counts, types, and assigned-on dates. The standards listed are:

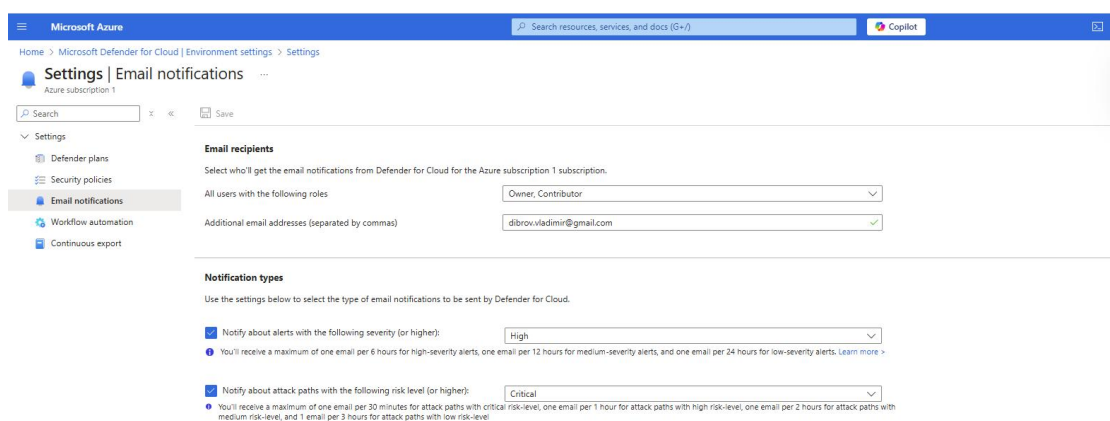
Name	Recommendations	Type	Assigned on	Status
Microsoft cloud security benchmark	225	Default	Subscription	On
NIST SP 800-171 Rev. 2	446	Compliance	Subscription	On
CIS Controls v8.1	182	Compliance	Subscription	On
CIS Microsoft Azure Foundations Benchmark v2.0.0	205	Compliance	-	Off
Spain ENS	859	Compliance	-	Off
NIST SP 800-53 Rev. 5	702	Compliance	-	Off
NIST CSF v2.0	112	Compliance	-	Off



The screenshot shows the 'Recommendations' page in the Microsoft Azure portal. The page displays a summary of recommendations by risk level and a table of specific recommendations. The summary shows 3 Critical, 12 High, 23 Medium, and 133 Low risk recommendations. The table lists the following recommendations:

Title	Affected resource	Risk level	Risk factors	Attack paths	Owner	Status	Insights
Storage accounts should restrict network access using virtual network rules	andribeasha96b	Critical	Critical Resource	0		Unassigned	
Storage accounts should prevent shared key access	andribeasha96b	Critical	Critical Resource	0		Unassigned	
Storage accounts should use a private link connection	andribeasha96b	Critical	Critical Resource	0		Unassigned	
Container registries should use private link	devregistry20230126	High	Lateral Movement	0		Unassigned	
Container registries should not allow unrestricted network access	devregistry20230126	High	Lateral Movement	0		Unassigned	
Storage accounts should prevent shared key access	denisistorageacc	Medium	Exposure to the Internet	0		Unassigned	
Storage accounts should prevent shared key access	hstate20640	Medium	Exposure to the Internet	0		Unassigned	
Storage accounts should prevent shared key access	hstatestorage2025dev	Medium	Exposure to the Internet	0		Unassigned	
Storage accounts should prevent shared key access	backendstorage598173	Medium	Exposure to the Internet	0		Unassigned	

3.Configured alerts for security incidents and integrate them with Azure DevOps using



The screenshot shows the 'Settings | Email notifications' page in the Microsoft Azure portal. The page is titled 'Email recipients' and 'Notification types'. The 'Email recipients' section shows that notifications are sent to all users with the following roles: Owner, Contributor. The 'Notification types' section shows that notifications are sent for alerts with the following severity: High, and for attack paths with the following risk level: Critical.

Azure Logic Apps or Azure Functions.

- Create an Azure DevOps work item automatically when a security alert is triggered.

Home > LogikAppDibrova | Workflows > JustWorkflow | Designer

Workflow

Search

Tools

- Designer
- Code
- Run history
- Configuration
 - Properties
 - Settings
 - Access keys

Run

Save

Discard

Parameters

Code view

Errors

Assistant

Workflow summary

Log stream

Info

File a bug

Create a work item

Parameters

Settings

Code view

Testing

About

Organization Name *

VolodymyrDibrova0326

Project Name *

MyProjectVivi

Work item Type *

Issue

Title *

Security Alert: [properties.alertDisplay...]

Description

Normal

Arial

15px

B

I

U

A

on

Alert Details: [properties.description...]

Advanced parameters

Showing 0 of 11

Show all

Clear all

Connected to ConnectDevAzure

Change connection

Home > LogikAppDibrova | Workflows > JustWorkflow | Run history

Workflow

Search

Run

Refresh

Set as default page

Tools

- Designer
- Code
- Run history
- Configuration
 - Properties
 - Settings
 - Access keys

Essentials

Run history

Trigger history

Add filter

Identifier	Status	Start time (Local Time)	Fired
08584604934421113079194042454CU00	Succeeded	3/4/2025, 8:37:23 PM	
08584604943785667480398270481CU00	Succeeded	3/4/2025, 8:21:46 PM	
08584604945243251640057264986CU00	Succeeded	3/4/2025, 8:19:21 PM	
08584604945266207491718026255CU00	Succeeded	3/4/2025, 8:19:18 PM	

Azure DevOps

VolodymyrDibrova0326

MyProjectVivi

Boards

Work items

Work items

Recently created

New Work Item

Open in Queries

Column Options

Import Work Item

Filter by keyword

ID	Title	Assigned To
9	Backend Manual Tests	Volodymyr Dibrova
7	Frontend Manual Tests	Volodymyr Dibrova
6	FullstackApp Test Plan	Volodymyr Dibrova
5	FullstackApp Test Plan	Volodymyr Dibrova
4	FullstackApp Test Plan	Volodymyr Dibrova
3	first test case	Volodymyr Dibrova
2	My Test Plan 1	Volodymyr Dibrova
1	My Test Plan 1	Volodymyr Dibrova

Task 3: Implementing a Comprehensive DevSecOps Strategy with Azure Policy and Automation

Objective: Implement a comprehensive DevSecOps strategy using Azure Policy, Azure Blueprints, and automation to enforce security best practices, ensure compliance, and streamline governance across your Azure environments.

Steps:

- **Create Azure Policies:**

Navigate to the Azure Portal and go to "Policy." Create or select existing policies that enforce security best practices, such as requiring encryption at rest, ensuring secure network configurations, or enforcing tag usage for resources. Assign these policies to your Azure subscriptions or resource groups to start auditing resources for compliance.

- **Set Up Azure Blueprints:**

In the Azure Portal, go to "Blueprints." Create a new blueprint definition that includes your Azure Policies, resource templates, and RBAC assignments. Publish and assign the blueprint to your target subscriptions to ensure consistent deployment of resources and policies.

- **Automate Compliance Monitoring:**

Use Azure Monitor to set up alerts for policy compliance states. Configure Log Analytics to collect and analyze data on policy compliance, creating dashboards to visualize this data.

- **Implement Automated Remediation:**

Use Azure Automation or Azure Functions to create runbooks or scripts that automatically remediate common policy violations, such as enabling encryption or applying missing tags. Trigger these runbooks based on alerts from Azure Monitor when policy violations are detected.

- **Configure Role-Based Access Control (RBAC):**

Go to "Access control (IAM)" in the Azure Portal for your resources. Assign roles that adhere to the principle of least privilege, ensuring users have only the permissions they need. Regularly review role assignments and adjust as necessary based on access requirements.

- **Integrate with Azure DevOps:**

Set up Azure DevOps pipelines to include policy compliance checks using Azure CLI or Azure PowerShell tasks. Use these tasks to ensure that resources deployed through the pipeline are compliant with your defined policies.

- **Test and Validate the Implementation:**

Deploy a test resource using your blueprint and verify that all policies are applied

and compliant. Simulate a policy violation and test the automated remediation process to ensure it works as expected.

Create Azure Policies and Assigned

Microsoft Azure

Home > Policy | Definitions > myPolicy >

myPolicy

Edit Policy definition

```
1  {
2    "mode": "All",
3    "policyRule": {
4      "if": {
5        "allOf": [
6          {
7            "field": "Microsoft.Compute/diskEncryptionSettingsCollection.enabled",
8            "equals": "[parameters('encryptionRequired')]"
9          },
10         {
11           "field": "location",
12           "in": "[parameters('allowedLocations')]"
13         }
14       ],
15       "then": {
16         "effect": "deny"
17       }
18     },
19     "parameters": {
20       "encryptionRequired": {
21         "type": "Boolean",
22         "metadata": {
23           "displayName": "Require encryption",
24           "description": "Ensures all disks are encrypted"
25         },
26         "defaultValue": true
27       },
28       "allowedLocations": {
29         "type": "Array",
30         "metadata": {
31           "displayName": "Allowed locations",
32           "description": "List of allowed locations for disk creation"
33         },
34         "defaultValue": []
35       }
36     }
37   }
38 }
```

Home > Policy

Policy | Compliance

Search

Assign policy Assign initiative Refresh

Overview

Getting started

Compliance

Remediation

Events

Authoring

Definitions

Assignments

Exemptions

Search

Filter by name or ID...

Scope: Azure subscription 1 Definition type: All definition types Compliance state: All compliance states

Overall resource compliance 8% 22 out of 274

Resources by compliance state 274

22 - Compliant 252 - Non-compliant

Non-compliant initiatives 4 out of 7

Non-compliant resource compliance 148 out of 274

Name	Scope	Compliance state	Resource compliance	Non-compliant resources	Non-compliant policies
task03ba	Azure subscription 1	Non-compliant	13% (34 out of 256)	222	1
CIS Controls v8.1	Azure subscription 1	Non-compliant	39% (104 out of 269)	165	55
NIST SP 800-171 Rev. 2	Azure subscription 1	Non-compliant	32% (35 out of 109)	74	50
Microsoft cloud security benchmark	Azure subscription 1	Non-compliant	27% (16 out of 60)	44	40
Task2 [Assigned by MDC]	Azure subscription 1	Non-compliant	0% (0 out of 19)	15	2
myPolicy	Azure subscription 1	Compliant	100% (14 out of 14)	0	0
ASC DataProtection (subscription: 9afae438-d8c3-444e-b0f2)	Azure subscription 1	Compliant	100% (1 out of 1)	0	0
Audit untagged storage account	Azure subscription 1/VulliaHrabovenko	Compliant	100% (2 out of 2)	0	0
Defender for SQL on SQL VMs and Arc-enabled SQL Servers	Azure subscription 1	Compliant	100% (0 out of 0)	0	0
EnforceDSC	Azure subscription 1	Compliant	100% (0 out of 0)	0	0
ASC OpenSourceRelationalDatabaseProtection (subscription: 9afae438-d8c3-444e-b0f2)	Azure subscription 1	Compliant	100% (0 out of 0)	0	0

Set Up Azure Blueprints

Microsoft Azure

Home > Blueprints

Blueprints | Blueprint definitions

Search

Create blueprint Refresh

On July 11, 2026, Blueprints (Preview) will be deprecated. Migrate your existing blueprint definitions and assignments to Template Specs and Deployment Stacks. For more details on how to migrate, go to <https://aka.ms/AzureBlueprintMigrate>.

Scope: Azure subscription 1

Blueprints: All

Search by blueprint name

Name	Latest Version	Unpublished changes	Last modified	Definition location
blueprint3	1.0	No	3/1/2023	Azure subscription 1
DevSecOps-Blueprint-Dibrová	v4	No	3/4/2023	Azure subscription 1
task03blueprint	0.1	No	3/1/2023	Azure subscription 1

Microsoft Azure

All services > Blueprints > Blueprint definitions > DevSecOps Blueprint: Dibraova >

Assign blueprint

On July 11, 2026, Blueprints (Preview) will be deprecated. Migrate your existing blueprint definitions and assignments to Template Specs and Deployment Stacks. For more details on how to migrate, go to <https://aka.ms/AzureBlueprintNotice>.

Blueprint definition version * ⓘ
v8

Lock Assignment ⓘ
[Don't Lock](#) [Do Not Delete](#) [Read Only](#)

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources. [Learn more](#)

Managed Identity ⓘ
☒ System assigned
☐ User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all artifacts. We will automatically remove this access when the blueprint assignment process is finished.

Artifact parameters

Artifact / Parameter	Parameter Value
<input checked="" type="checkbox"/> Subscription	
<input checked="" type="checkbox"/> myPolicy	
Require encryption (Policy: myPolicy)	true
Allowed Locations (Policy: myPolicy)	8

[Assign](#) [Cancel](#)

Microsoft Azure

All services > DevSecOps Blueprint: Dibraova >

Assign blueprint

On July 11, 2026, Blueprints (Preview) will be deprecated. Migrate your existing blueprint definitions and assignments to Template Specs and Deployment Stacks. For more details on how to migrate, go to <https://aka.ms/AzureBlueprintNotice>.

[Don't Lock](#) [Do Not Delete](#) [Read Only](#)

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources. [Learn more](#)

Managed Identity ⓘ
☒ System assigned
☐ User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all artifacts. We will automatically remove this access when the blueprint assignment process is finished.

Artifact parameters

Artifact / Parameter	Parameter Value
<input checked="" type="checkbox"/> Subscription	
<input checked="" type="checkbox"/> [User group or application name] : Contributor	
[User group or application name] (User group or application name) : Contributor	Volodymyr Dibraova (VolodymyrDibraova@dmymtroshchinsky@gmail.com)
<input checked="" type="checkbox"/> [User group or application name] : Reader	
[User group or application name] (User group or application name) : Reader	Volodymyr Dibraova (VolodymyrDibraova@dmymtroshchinsky@gmail.com)
<input checked="" type="checkbox"/> myPolicy	
Require encryption (Policy: myPolicy)	true
Allowed Locations (Policy: myPolicy)	8

[Assign](#) [Cancel](#)

Blueprint assignment failed
Blueprint assignment "Assignment-DevSecOps-Blueprint-Dibraova" failed for subscription "9afae42b-0bc2-44fe-b0d2-4e0839267a07". Azure Blueprints was unable to obtain owner permissions for the specified subscription.
[Help me troubleshoot](#)

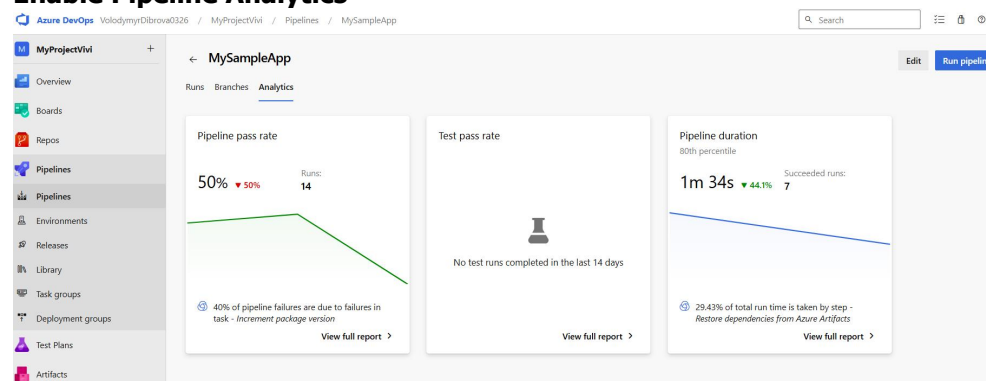
Issue: I cannot continue the task because I don't have Contributor permissions on the subscription. Azure Blueprints requires Contributor access to assign policies and deploy resources. Without this permission, the assignment fails.

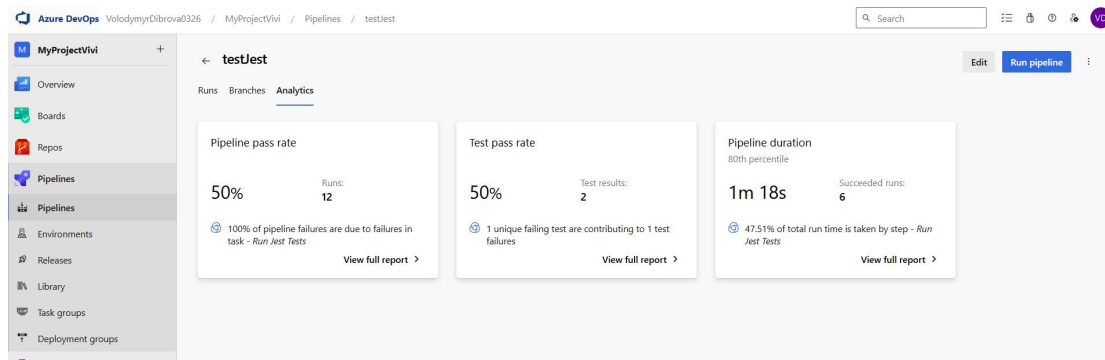
Task 4: Monitoring DevOps Pipelines for Health and Performance

Objective: Set up a monitoring solution to track the health and performance of your Azure

DevOps pipelines, ensuring timely detection and resolution of issues to maintain efficient CI/CD processes.

Enable Pipeline Analytics





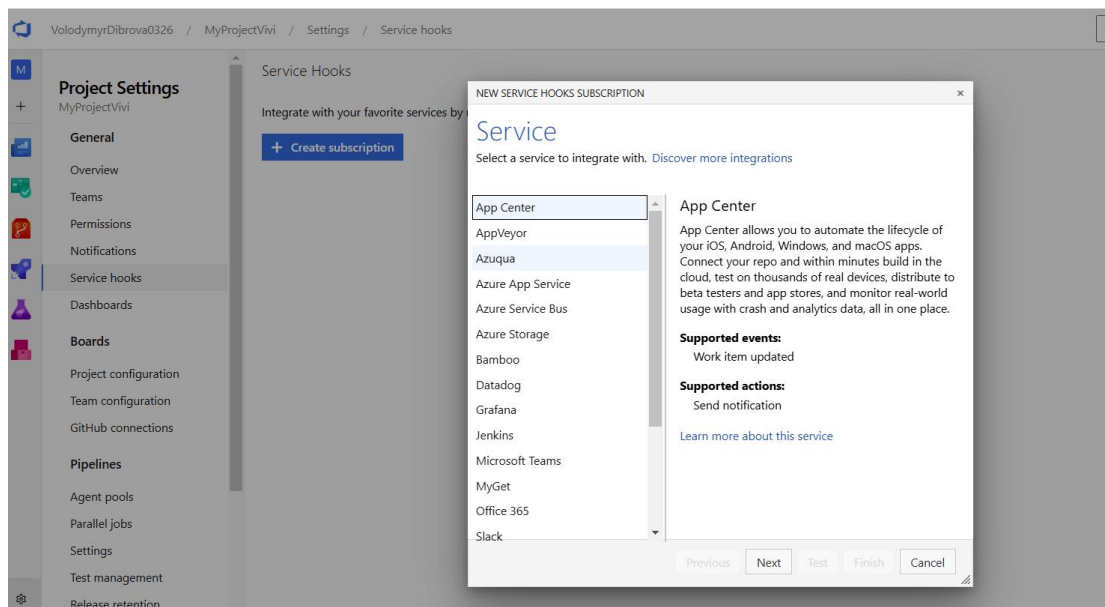
Integrate Azure Monitor for Logs

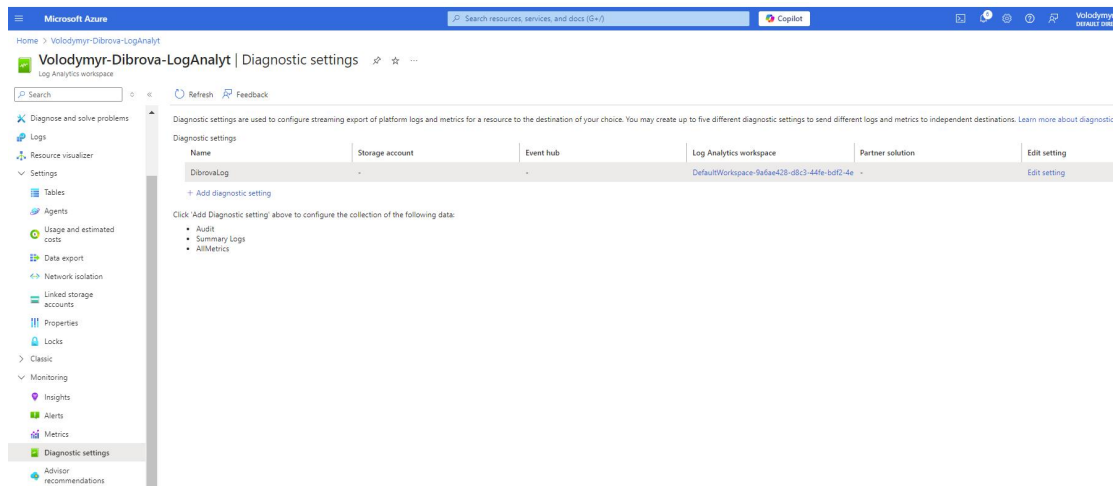
I tried to add a new Azure Monitor (Log Analytics) service to Service Hooks.

Then I would connect to Log Analytics in the Azure portal

But:

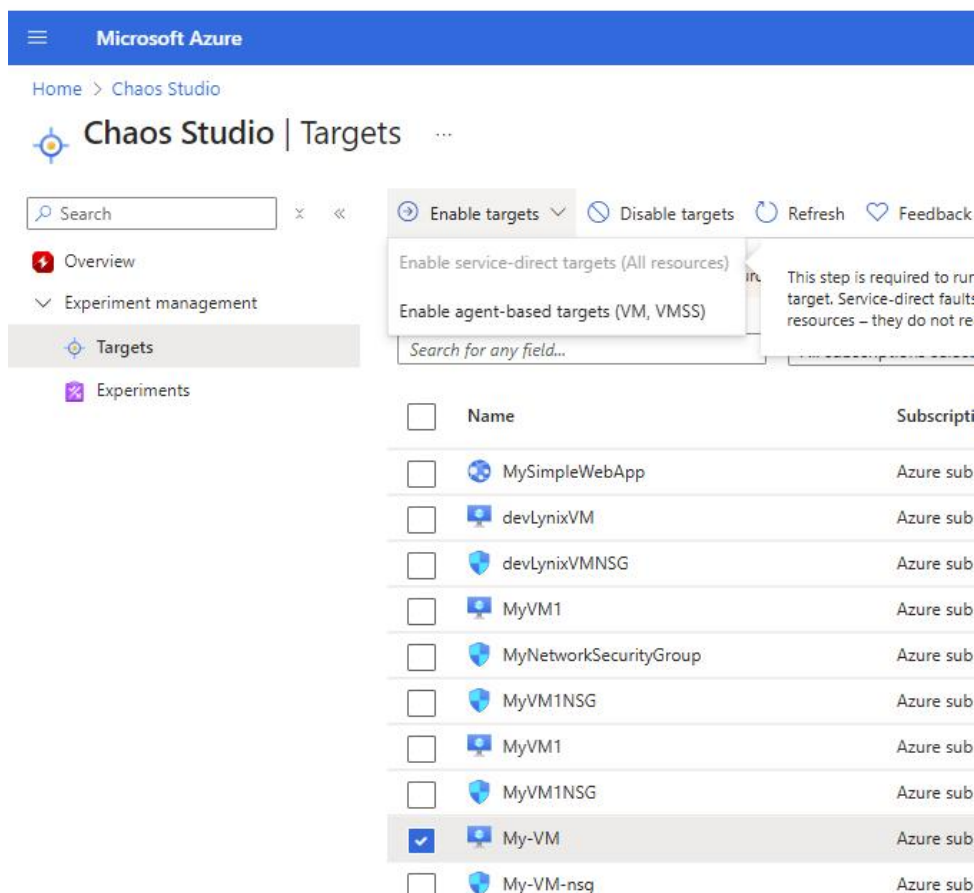
This means that the Azure DevOps Services Connector for Azure Monitor is not available, I don't have the required "Organization Owner" access rights.





Task 5: Implementing Chaos Engineering in Azure with Azure Chaos Studio
Objective: Use Azure Chaos Studio to conduct chaos experiments on Azure resources, testing the resilience of your applications and infrastructure to improve their reliability and stability.

Enabled target



Created Experiment and start

Home > Chaos Studio | Experiments > myChaosDibrova1 >

Edit experiment

Configure your experiment below. [Learn more](#)

Step 1
1 branch, 1 action, 1 target

Step *

Branch *

Step 1

Branch 1

Action	Parameter	Target resources	Scope
VM Shutdown	duration: 5 minutes abruptShutdown: false	1 resources	-

+ Add action

Add branch

Add step

Provide feedback

Did you find what you needed? Let us know how it went.

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Volodymyr.Dibrova@dm...
account select your partners

Chaos Studio | Experiments

Home > Chaos Studio | Experiments >

myChaosDibrova

Filter for any field...

Name ?

myChaosDibrova

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Locks

Identity

Monitoring

Alerts

Metrics

Diagnostic settings

Logs

Automation

Help

Essentials

Resource group (move) : Volodymyr-Dibrova

Subscription (move) : Azure subscription 1

Location (move) : East US

Tags (edit) : Add tags

Status : PreProcessing

Last started : 3/5/2023, 5:18:14 PM

Last ended : -

History

Start time	End time	Status	Identifier
3/5/2023, 5:18:14 PM	-	PreProcessing	CBF285A3-35F8-4EB7-8396-9- Details

Added access

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Volodymyr.Dibrova@dm...
account select your partners

My-VM | Access control (IAM)

Home > My-VM

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability > scale

Security

Backup > disaster recovery

Operations

Monitoring

Automation

Help

Number of role assignments for this subscription

146 4000

Vol

Type: All Role: All Scope: All scopes Group by: Role

Name	Type	Role	Scope	Condition
Contributor (2)				
Volodymyr.Dibrova@3236-MjProject@vic-35ae5-66621a2-406c-4fe9-abcc-49a0833de151	Service principal	Contributor	Subscription (Inherited)	None
Yoda@tuba-4001-4743-96a8-7852345a0e9f6c	Service principal	Contributor	Resource group (Inherited)	None
Chaos Studio Experiment Contributor (1)				
Volodymyr.Dibrova e654e6d2-099d-40d8-812c-3f80403aaf5c	User	Chaos Studio Experiment Contributor	Subscription (Inherited)	None
Log Analytics Contributor (1)				
Volodymyr.Dibrova e654e6d2-099d-40d8-812c-3f80403aaf5c	User	Log Analytics Contributor	Resource group (Inherited)	None
Monitoring Contributor (2)				
Volodymyr.Dibrova e654e6d2-099d-40d8-812c-3f80403aaf5c	User	Monitoring Contributor	Subscription (Inherited)	None
Volodymyr.Dibrova e654e6d2-099d-40d8-812c-3f80403aaf5c	User	Monitoring Contributor	Resource group (Inherited)	None
Virtual Machine Contributor (1)				
Volodymyr.Dibrova e654e6d2-099d-40d8-812c-3f80403aaf5c	User	Virtual Machine Contributor	This resource	None

Showing 1 - 7 of 7 results.

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > Chaos Studio | Experiments > myChaosDibrova1 >

myChaosDibrova1

Details

Refresh Feedback

The target resource(s) could not be resolved. Please verify that your targets exist and your managed identity has sufficient permissions on all target resources. Error Code: AccessDenied. Target Resource(s): Session ID: 4605d8c7af874136c99e8d552e6abb0b

Steps/Branches	Name	Status	Start time	End time	Duration
No steps/branches to display					

Issue: I cannot continue the task because I have problem with permissions on the subscription but I'm added.